

PORTABLE COMPUTER FORENSICS SOFTWARE TO ACQUIRE VOLATILE DATA

LIVE RESPONSE

Reveal the Truth: Volatile Data Collection from a USB Key

Live Response is the only USB key that enables first responders, investigators and IT security professionals to collect the live volatile data, which will be lost once the computer system is shut down. Acquire ALL volatile and requested data from a live system — in just minutes! Simply insert the USB key, and instruct the system to gather only the data you desire from a menu of options. Live Response will then collect and store the data directly onto the device within minutes. When you are finished, you can simply eject the USB key and walk away.

The logo for Live Response, featuring the words "Live Response" in a red, cursive font with a registered trademark symbol (®) at the end.

Data collected by Live Response®:

- Physical memory
- Network connections, open TCP or UDP ports, NetBIOS
- Currently logged on user / user accounts
- Current executing processes and services
- Scheduled jobs
- Windows registry
- Browser auto-completion data, passwords
- Screen capture
- Chat logs
- Windows SAM files / NTUser.dat files
- System logs
- Installed applications and drives
- Environment variables
- Internet history

With Live Response's easy-to-use graphical interface, investigators around the world can conduct computer forensics investigations quickly and easily.

- Acquire data including hidden or deleted items
- Store and transfer data easily

- Analyze data collected
- Review data collected
- Compile report with results

Contact

[Request Information](#)

Brochures

- [Live Response](#)

White Papers

- [LEGAL JOURNAL: The Rules of Evidence and AccessData Technology](#)
- [The Importance of Memory Search and Analysis](#)
- [MORE >](#)

[Go To Top »](#)

Products

- [Forensic Toolkit](#)
- [AD Enterprise](#)
- [AD eDiscovery](#)
- [AD Summation iBlaze](#)
- [AD Summation Enterprise](#)
- [AD Summation CaseVantage](#)
- [CIRT](#)
- [SilentRunner Sentinel](#)
- [AD Lab](#)
- [Mobile Phone Examiner Plus](#)
- [Distributed Network Attack](#)
- [Password Recovery Toolkit](#)

Support

- [AD Downloads](#)
- [Previous Releases](#)
- [Discussion Forum](#)

- [Technical Papers](#)

Resource Library

- [Brochures](#)
- [White Papers](#)
- [Webinars](#)

Training

- [AccessData Bootcamp](#)
- [AccessData Forensics](#)
- [Windows Forensics 7](#)
- [FTK 3 Transition Day](#)
- [Applied Decryption](#)
- [Internet Forensics](#)
- [Windows Forensics – XP](#)
- [Windows Forensics – Vista](#)
- [Windows Forensics – Registry](#)
- [Mobile Forensics 101](#)
- [Mobile Forensics 202](#)
- [Mobile Forensics 303](#)
- [MORE](#)

Contact Us

- [Americas/Asia Pacific](#)
- [Europe/Middle East/Africa](#)
- [Summation Software Support](#)
- [eDiscovery/Litigation Support Services](#)
- [Discovery Cracker Support](#)